

Настройка подключения OpenVPN.

Для подключения абонентов по протоколу OpenVPN, необходимо следующее:

- Создать корневой и конечный сертификаты в модуле Сертификаты. При создании конечного сертификата на вкладке «Использование ключа» в поле «Шаблон» следует выбрать значение «VPN-сервер».

Данные сертификата VPN-корневой

Общее

Название: VPN-корневой
Код страны: RU - Russian Federation
Имя или адрес хоста: test.ru

Настройки

Тип сертификата: CA
Алгоритм: SHA 256
Тип шифрования: RSA
Создан: 06.11.2019
Действует до: 07.11.2020
Длина ключа: 2048 бит

Использование ключа

Использование ключа: Certificate Sign
CRL Sign

Ок **Отмена**

Данные сертификата Openvpn-сервер

Общее

Название: Openvpn-сервер

Код страны: RU - Russian Federation

Имя или адрес хоста: test.ru

Настройки

Тип сертификата: Конечный сертификат

Алгоритм: SHA 256

Тип шифрования: RSA

Создан: 06.11.2019

Действует до: 07.11.2020

Длина ключа: 2048 бит

Использование ключа

Использование ключа: Digital Signature
Key Encipherment

Расширенное использование ключа: TLS Web Server Authentication

Netscape расширение: SSL Server

Ok

Отмена

- Добавить OpenVPN-сеть в модуле Провайдеры и сети. Для того, чтобы пользователи могли подключаться к ресурсам локальных сетей ИКС, необходимо установить флаг «Передать клиенту маршрут по умолчанию» и выбрать из списка сети, которые нужно маршрутизировать.

Добавление OpenVPN-сети

[Основные настройки](#) [Шифрование и сертификаты](#)

| | |
|--|--|
| Название * | Ip-адрес/Префикс * |
| <input type="text" value="Супер VPN"/> | <input type="text" value="10.8.0.0/24"/> |
| Протокол | Порт сервера * |
| <input type="text" value="UDP"/> | <input type="text" value="1194"/> |

Использовать NAT
 Разрешить трафик между клиентами
 Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей

 Муми-локалка (192.168.17.242/24) × ▼

Передать клиентам DNS сервера

Разрешить управление ИКС через веб
 Разрешить управление ИКС через SSH

Добавить Отмена

- В качестве сертификатов указать предварительно сгенерированные сертификаты из п.1.

Добавление OpenVPN-сети

[Основные настройки](#) [Шифрование и сертификаты](#)

| | |
|---|---|
| Алгоритм шифрования <input type="text" value="AES-256-CBC"/> <input type="button" value="▼"/> <input type="checkbox"/> Включить сжатие LZO | Алгоритм хеширования <input type="text" value="SHA256"/> <input type="button" value="▼"/> |
| link-MTU * <input type="text" value="1500"/> <input type="button" value="^"/> <input type="button" value="▼"/> | |
| Корневой сертификат * <input type="text" value="VPN-корневой"/> <input type="button" value="X"/> | Сертификат сервера * <input type="text" value="Openvpn-сервер"/> <input type="button" value="X"/> |

- Перейти в модуль VPN - Пользователи и отметить флагками пользователей, которым будет разрешено подключаться по протоколу OpenVPN, при этом будет предложено выбрать к какой из созданных сетей (если их несколько) будет подключаться пользователь. Важно: необходимо нажать кнопку «Сохранить», чтобы изменения вступили в силу.

Муми-дол > VPN-сервер > Пользователи Туве Янссон 19

| VPN-сервер | Настройки | Пользователи | Текущие сеансы | События | Журнал | |
|---|-------------------------|--|--|----------------|--------|--|
| Добавить <input type="button" value="▼"/> | Удалить | Выключить <input type="button" value="▼"/> | Редактировать | | | |
| Имя | Логин | Ip-адреса из Vpn-сетей | Vpn-доступ | OpenVPN-доступ | | |
| <input type="checkbox"/> Корневая группа <input checked="" type="checkbox"/> Муми-дол <input type="checkbox"/> Мумики Муми-мама Муми-папа Муми-троль (месячная квота исчерпана) <input type="checkbox"/> Спорки | mumi3 mumi2 mumi1 | | <input type="checkbox"/> <input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24) <input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24) <input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24) <input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24) | | | |

- Перейти в индивидуальный модуль пользователя, вкладка OpenVPN. Если необходимо настроить маршрутизацию из локальной сети ИКС до других ресурсов в локальной сети

пользователя, то необходимо прописать сеть, в которой находится данный пользователь.

The screenshot shows the 'User' section with the 'OpenVPN' tab selected. A message at the top states: 'OpenVPN-доступ для пользователя включен в Супер VPN (10.8.0.0/24)'. Below this, there is a checkbox labeled 'Передать клиенту маршрут по умолчанию'. Under 'Передать клиентам маршруты до сетей', there is a dropdown menu set to 'Передать клиентам маршруты до сетей' and a text input field containing '192.168.0.1/24'. Under 'Сертификат клиента*', a dropdown menu shows 'Супер VPN_Муми-папа'. At the bottom, there are three buttons: 'Сохранить' (green), 'Обновить', and 'Выгрузить сертификаты'.

- В модуле Провайдеры и сети необходимо выгрузить архив (openvpn-configs.tar.gz) с пользовательскими сертификатами (*.ovpn) для их подключения. Или каждый Пользователь должен самостоятельно зайти в свой личный кабинет и скачать свой сертификат, в формате *.ovpn.

The screenshot shows the 'Providers and networks' section. It lists four entries: 'Моррателеком (192.168.170.242/24)', 'Муми-локалка (192.168.17.242/24)', 'Вай-фай (192.168.242.242/24)', and 'Супер VPN (10.8.0.0/24)'. The 'Супер VPN' entry is highlighted. Its details are shown below: Ip-адрес/Префикс: 10.8.0.0/24, Протокол: udp, Порт сервера: 1194, Корневой сертификат: VPN-корневой, Сертификат сервера: Openvpn-сервер. At the bottom, there are buttons for 'Подробнее...', 'Настройки авторизации', 'Выгрузить сертификаты', 'Удалить', 'Редактировать', and 'Выключить'.

- Для подключения пользователя, ему необходимо установить на своем компьютере утилиту OpenVPN (<https://openvpn.net/>), запустить ее и импортировать файл *.ovpn. После этого станет доступным возможность подключения.

- В случае использования иной утилиты подключения к OpenVPN серверу и требования иметь файлы: ca.crt, client.crt, client.key, ta.key. Необходимо создать их вручную и наполнить информацией из файла *.ovpn (более подробная инструкция наполнения [файлов](#), пункты 4 и 5).

Прекращение доступа Пользователя к OpenVPN

Для того чтобы отозвать у Пользователя доступ к OpenVPN, необходимо перейти в Меню - Сеть - VPN - вкладка «Пользователи», напротив необходимого Пользователя снять флаг «OpenVPN-доступ» и нажать «Сохранить». При этом доступ у Пользователя прекратиться сразу, даже если у него было активное соединение. В Меню - Защита - Сертификаты, созданный ранее автоматический сертификат Пользователя, будет серым с состоянием «сертификат отозван». **ВНИМАНИЕ:** отозванный сертификат не рекомендуется удалять из модуля «Сертификаты», иначе этот сертификат пропадёт из списка отозванных и Пользователь с таким сертификатом вновь получит доступ к OpenVPN. При удалении Пользователя из «ИКС», который имеет доступ к OpenVPN, его сертификат будет также отозван.

| | | | | | |
|-------------------------|---------------------|---------------|------------|------------|---------|
| CAaaaa | CA | не зашифрован | 14.04.2020 | 15.04.2021 | test.ru |
| ServerVPN | Конечный сертификат | не зашифрован | 14.04.2020 | 15.04.2021 | test.ru |
| Новая OpenVPN-сеть_OVPN | Конечный сертификат | не зашифрован | 14.04.2020 | 16.04.2021 | ttttt |
| Новая OpenVPN-сеть_OVPN | Конечный сертификат | не зашифрован | 14.04.2020 | 15.04.2021 | ttttt |

From:
<https://doc-old.a-real.ru/> - **Документация**



Permanent link:
https://doc-old.a-real.ru/doku.php?id=ics70:openvpn_setup&rev=1589981002

Last update: **2020/05/20 16:23**